Alhaqbani, Bandar S. and Fidge, Colin J. (2009) ***A time-variant medical data trustworthiness assessment model.*** In: Proceedings of the 11th International Conference on e-Health Networking, Applications and Services, 15-18 December 2009, Sydney.

A Time-Variant Medical Data Trustworthiness Assessment Model

Bandar Alhaqbani
Information Security Institute
Queensland University of Technology
Brisbane, Australia
Email: b.alhaqbani@isi.qut.edu.au

Colin Fidge
Faculty of Science and Technology
Queensland University of Technology
Brisbane, Australia
Email: c.fidge@qut.edu.au

***Abstract*—Electronic Health Record (EHR) systems are being introduced to overcome the limitations associated with paper-based and isolated Electronic Medical Record (EMR) systems. This is accomplished by aggregating medical data and consolidating them in one digital repository. Though an EHR system provides obvious functional benefits, there is a growing concern about the privacy and reliability (trustworthiness) of Electronic Health Records. Security requirements such as confidentiality, integrity, and availability can be satisfied by traditional hard security mechanisms. However, measuring data trustworthiness from the perspective of data entry is an issue that cannot be solved with traditional mechanisms, especially since degrees of trust change over time. In this paper, we introduce a Time-variant Medical Data Trustworthiness (TMDT) assessment model to evaluate the trustworthiness of medical data by evaluating the trustworthiness of its sources, namely the healthcare organisation where the data was created and the medical practitioner who diagnosed the patient and authorised entry of this data into the patient's medical record, with respect to a certain period of time. The result can then be used by the EHR system to manipulate health record metadata to alert medical practitioners relying on the information to possible reliability problems.**

I. Introduction

The healthcare domain—as one of the world's largest hybrid organisations—stands to gain enormously from the increased adoption of Information and Communications Technologies. Electronic Health Record (EHR) systems are the latest evolution of healthcare ICT.

Electronic Health Records can enable efficient communication of medical information, and thus reduce costs and administrative overheads [1], [4]. However, to achieve these potential benefits, the healthcare industry needs to overcome several significant obstacles, in particular concerns about the trustworthiness (reliability) of EHR medical data. Trustworthiness is a crucial factor that has a strong effect on how medical practitioners use data [5]. This concern is raised because EHR data is composed from different healthcare providers' Electronic Medical Record (EMR) systems, from paper-based medical reports and from referrals that patients get from those healthcare providers who do not have an EMR system or an electronic connection with the EHR system. By using an EHR system, a medical practitioner will thus be exposed to historical medical data with varying levels of reliability; the data might originate from a healthcare organisation that does not satisfy patient safety requirements, e.g. is known to habitually enter inaccurate or incomplete data, or be entered by a medical practitioner who fails to satisfy medical guidelines, e.g. is known to violate medical procedures. As a consequence, the trustworthiness of EHR data depends on the trustworthiness of its source and creator. In order to measure the trustworthiness of an agent, reputation systems [13], [14] provide an accumulative trustworthiness measure of an agent where all past experiences and/or feedback about the agent are combined. Most reputation systems are built to assess the trustworthiness of an agent at the present time. In other words they provide the expected future behaviour of an agent based on its current trustworthiness. However, they do not provide a way to assess an agent's trustworthiness at a particular time in the past. Evaluating the trustworthiness of past entries is crucial in the healthcare domain where a medical history combines *historical* medical data.

To illustrate this requirement, consider the following example. Assume that in year 2009 Hospital A's EHR system received two medical reports, Patient Y's diagnosis and Patient Z's prescription, that were created by Dr X in 2000 and 2005 respectively. The EHR system maintains a database where it stores its observed experiences with external agents. It uses an

TABLE I
The EHR's observed trustworthiness of Dr X

Time	Number of observed experiences		Trustworthiness
	Good	Bad	
1999	1	1	0.5
2000	2	0	0.75
2001	3	0	0.85
2002	1	6	0.5
2003	0	7	0.33
2004	0	7	0.25
2005	0	5	0.21
2006	1	0	0.23
2007	6	0	0.35
2008	5	0	0.42
2009	6	1	0.48

* B. Alhaqbani and C. J. Fidge. A time-variant medical data trustworthiness assessment model. In D. Hoang and M. Foureur, editors, *Proceedings of the 11th International Conference on e-Health Networking, Applications and Services (HealthCom 2009), 16-18 December, Sydney*. IEEE, December 2009. *To appear*.

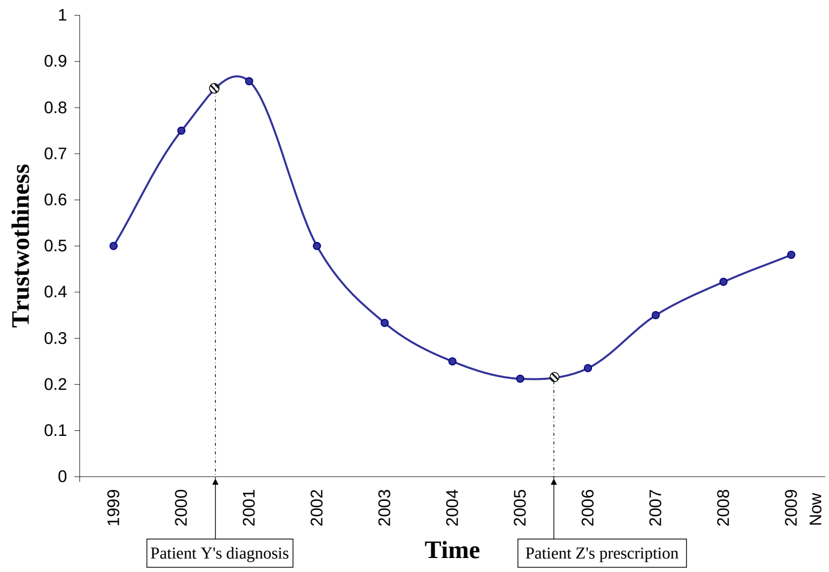


Fig. 1. The EHR's continuous trustworthiness measurement of Dr Tony

eBay-like reputation system (though this is not an appropriate mechanism as we will see in Section II) in which it records the number of observed good and bad experiences with an agent per annum and uses this to calculate a cumulative trust measure (Table I). In this case, these good and bad experiences are generated from previously evaluated medical entries that were created by Dr X. Correct diagnoses and accurately following medical procedures are examples of good experiences whereas misdiagnoses, incomplete or careless data entry, and failure to follow medical procedures are bad events. Fig. 1 represents the observed trustworthiness of Dr X that Hospital A maintains over time.

Now, let's see how Hospital A will evaluate the trustworthiness of the received two medical reports. In current reputation systems, the calculated trustworthiness value of Dr X in the year 2009 will be used as the trustworthiness of the two medical records, however this is an inaccurate measure because it represents Dr X's expected future behaviour instead of his previous behaviour at the time the records were created. From Fig. 1, we notice that Patient Y's diagnosis was created at a time period when Dr X was evaluated to be trustworthy, whereas Patient Z's prescription was written during a time period when Dr X was believed to be untrustworthy. Therefore, assigning the trustworthiness value that is calculated in year 2009 to these two medical records is inappropriate due to the fact that trustworthiness is a dynamic attribute and varies according to Dr X's behaviour as shown in Fig. 1.

Another approach is to consider Dr X's absolute trustworthiness value in 2000 and 2005 for these two records. Although this approach provides a better estimate, it does not consider the dynamic behaviour of the trustworthiness attribute. For example, between 1999 and 2001, inclusive, Dr X was believed to be providing trustworthy medical data. However in 2002 he has been shown not to follow appropriate medical procedures in his diagnosis of a particular case, and this error has been detected more than once. Therefore, this change of Dr X's trustworthiness will have an impact on his immediately preceding data entries, and the same thing can be said about the impact of his previous trustworthiness behaviour on the following medical data entries.

In this paper, we introduce a Time-Variant Medical Data Trustworthiness assessment (TMDT) model to assist the EHR system to validate the trustworthiness of received/stored medical data. The TMDT model uses a statistical approach that depends on the observed experiences available to the EHR system and its context assumptions. In order to provide an accurate trustworthiness estimate for historical medical data, we consider a time period that defines the trustworthiness assessment's time scope around the time when the data was produced. The defined time scope enables our model to capture the dynamic behaviour of the agent's trustworthiness. To conduct this assessment we use medical metadata to extract information about the medical data sources (e.g. timestamps, healthcare agents, and medical practitioners) and, thereafter, this information is used in a statistical process to derive the trustworthiness value of the medical data. The result can then be expressed in the health record by manipulating the EHR's metadata to alert the medical practitioner to possible reliability problems.

II. Related Work

Reputation systems provide a useful approach to assess the trustworthiness (or reliability) of a certain agent or service. These systems provide a reputation score for an agent calculated from the agent's ratings as voted on by others who have experienced a transaction with the agent. For instance, eBay's[1] feedback forum is one of the earliest online reputation systems; it collects buyers' feedback (either $+1$, 0, or -1) and aggregates them equally [10] to produce a global reputation score for the seller. The global score is further processed to provide the percentage of positive feedback gained by the seller. However, this additive scheme ignores the personalised nature of reputation measures [9]. It merely produces a sum of all historical behaviour and does not provide a view of behaviour at particular times in the past. A slightly better approach, the average reputation scheme [11], provides an improved calculation because it computes the reputation score as the average of all ratings. This principle is used in the reputation systems of many commercial web sites, such as Revolution Health[2] and Amazon[3]. Although the averaging reputation scheme is better than the additive scheme, it still has the same weaknesses.

In Peer-to-Peer (P2P) research, many reputation models have been proposed to assist in assigning reputation scores to those agents within the P2P network. These scores help an agent (service seeker) to make its own decision to trust and connect to the most honest and reliable agents (service providers). EigenTrust [8] is a reputation-based trust management system that aims to minimise malicious behaviour in a peer-to-peer network. It computes the agents' trust scores through repeated and iterative multiplication and aggregation of trust scores along transitive chains until the trust scores for all agent members of the P2P community converge to stable values. PeerTrust [13], [14] is another reputation-based trust management system for P2P eCommerce communities. It is even more cautious and examines the received ratings for their quality. It uses five factors to do so, namely feedback in terms of the amount of satisfaction, the number of transactions, the transaction's context factor, and the community context factor. These factors are used to discount the agent's trust value. However, our work differs from these two models in two respects. Firstly, in the healthcare context, it's crucial to have on hand the identity of the agent who created the medical data (i.e. the healthcare provider or medical practitioner) in order to ensure accountability. In this way, the healthcare context differs significantly from the P2P context. Secondly, in our model we follow a sounder time-variant and context-dependant mathematical basis that uses beta and dirichlet probability density functions for combining feedback and for expressing reputation scores, which makes our model capable of evaluating the trustworthiness of historical data that the former two models fail to achieve.

Beta and dirichlet probability density functions are used widely in the reputation arena [3], [6], [7], [12] to compute reputation scores in order to predict the expected future behaviour of an agent. However, they have not been employed to evaluate an agent's expected behaviour at particular times in the past. Therefore, our model extends these approaches to enable the evaluation of an agent's reputation at a certain time in the past by considering a time period centered around the time at which an event occured.

[1] www.ebay.com
[2] www.revolutionhealth.com
[3] www.amazon.com

III. Time-Variant Medical Data Trustworthiness (TMDT) Assessment Model

Let's assume a healthcare agent ha has received (or has) medical data md about a specific patient p, and that md consists of medical data fields *mdfs* and each $mdf \in$ *mdfs* has attached metadata $meta$. This metadata provides information about the source healthcare organisation src where mdf was created, and it reveals the identity mp of the medical practitioner who diagnosed patient p and authorised entry of data mdf into p's medical record. In addition, the metadata records the timestamp t of the lodged mdf.

In order for agent ha to evaluate the trustworthiness $T^t_{ha,mdf}$ of a given medical data field mdf at time t, it conducts a trustworthiness assessment for those agents who produced the mdf data. It evaluates the trustworthiness of the source healthcare organisation src and the medical practitioner mp at time t, denoted $AT^t_{ha,ag}$, where $ag \in \{src, mp\}$. Also, it employs the legal agent ag's medical misconduct practice rate MR_{ag} which affects our trust in medical data field mdf if it appears that ag has had any medical malpractice cases. Finally, healthcare agent ha substitutes this information in Eq. 1 to produce a trustworthiness measure for medical data field mdf which produces values between 0 (not-trusted) and 1 (fully-trusted).

$$T^t_{ha,mdf} = \sum_{ag \in AG} \xi_{ag} AT^t_{ha,ag} \times \sum_{ag \in AG} \omega_{ag} MR_{ag}$$
$$\text{where} \begin{cases} AG = \{src, mp\} \\ \sum_{ag \in AG} \omega_{ag} = 1 \\ \sum_{ag \in AG} \xi_{ag} = 1 \end{cases} \tag{1}$$

Here ξ_{src} and ξ_{mp} are weighting factors that are set by the healthcare agent ha to express the importance that ha puts on the trustworthiness of the roles of the source healthcare agent and medical practitioner. Also, ω_{src} and ω_{mp} are weighting factors that denote the significance that ha puts on received medical misconduct rates for these two agents.

In the following sections, we show the calculation process for the terms in Eq. 1.

A. Trustworthiness Evaluation

In the TMDT model, we follow two approaches in calculating the trustworthiness of a given agent $ag \in AG$ at time t, and this approach is determined by evaluating confidence criteria. In this model, we define the confidence criteria as the number of interaction experiences n with agent ag during period T. The time scope T is determined by using a fixed offset per to be the interval $[t - per, t + per]$ in order to capture the dynamic behaviour of the agent's trustworthiness. Offset per is set by the EHR system's administrator and can be changed at any time. The size of per influences our assessment's final result as we show in Section IV.

However, based on the criteria, healthcare agent ha will use its own internal assessment approach if its direct interaction experiences with agent ag within period T is greater than or equal to n, otherwise it will use an external assessment where it will seek assistance from neighboring agents and use information generated from reputation systems (Figure 2).

1) Internal Assessment: Healthcare agent ha uses its database that records good and bad historical experiences with agents including healthcare organisations and medical practitioners. These experiences are represented in a binary format, $E_{ha,ag}$, where $E_{ha,ag} = 1$ implies that ha has a good experience with ag and $E_{ha,ag} = 0$ indicates a bad experience. During a specific time scope T, the history of experiences between agents ha and ag is recorded as a tuple, $E^T_{ha,ag} = \Big(\#\{t \in T | E^t_{ha,ag} = 1\}, \#\{t \in T | E^t_{ha,ag} = 0\}\Big)$. The probability $p(E^t_{ha,ag})$ that an agent ag has provided correct or trustworthy data at time t is governed by its behaviour function $B^T_{ha,ag}$ during period T.

$$p(E^t_{ha,ag} = 1) \overset{\text{def}}{=} B^T_{ha,ag}, \text{ where}$$
$$B^T_{ha,ag} \in [0,1] \quad \text{and} \quad T = [t - per, t + per]$$

From this point on, we use B to denote ag's perceived trust in data received by ha at time t.

In order to compute the trustworthiness of a given agent ag, we adopt a probabilistic approach to modeling trust, based on the recorded experiences with ag. If a healthcare agent ha has complete information about agent ag then, according to ha, the probability that ag has provided correct/trustworthy information is expressed by B. In general, however, complete information cannot be assumed, and according to the Bayesian view [2], the best we can do is to use the expected value of B given ha's knowledge. In particular, we consider ha's knowledge of agent ag to be the set of all experiences it has observed. However, in adopting a Bayesian rather than frequentist stance (e.g. as does eBay), we allow for the probability that ha may use other information in its assessment.

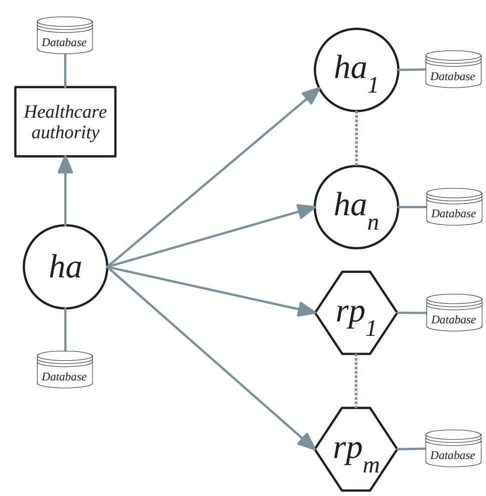


Fig. 2. Getting information from external sources

Therefore, we define ag's trustworthiness at time t according to ha as the expected behaviour of ag at time t given the set of ag's experiences that were recorded in the surrounding period T. This is expressed using standard statistical notation as shown in Eq. 2.

$$AT^t_{ha,ag} \overset{\text{def}}{=} E[B | E^T_{ha,ag}] \tag{2}$$

In order to determine this expected value, we need a probability distribution, defined by *a probability density function* (pdf), which is used to model the relative probability that B will have a certain value. In Bayesian analysis, the beta family of pdfs is commonly used as a prior distribution for a random variable that takes on continuous values in the interval $[0, 1]$. For example, beta pdfs can be used to model the distribution of a random variable representing the unknown probability of a binary event, where B is an example of such a variable. Therefore, beta pdfs have been applied in previous work in modeling trust [6].

The standard formula for beta distribution is expressed in Eq. 3, in which two parameters, α and β define the shape of the density function.

$$f(B_{ha,ag} | \alpha, \beta) \overset{\text{def}}{=} \frac{(B_{ha,ag})^{\alpha}(1 - B_{ha,ag})^{\beta-1}}{\int_0^1 U^{\alpha-1}(1-U)^{\beta-1}dU}, \quad \text{where } \alpha, \beta > 0 \tag{3}$$

In order to calculate the expected value of B, we need to define values for α and β that represent ha's belief about ag. With zero experiences with ag, ha believes that all possible values of B are equally likely, thus ha's initial values for α and β are $\alpha = \beta = 1$. These parameters are updated according to ha's observation about ag, where the value of α gets incremented by the number of good experiences $g^T_{ha,ag}$ that are recorded in time period T, and β gets increased by the number of bad experiences $b^T_{ha,ag}$ as in Eq. 4.

$$\alpha = g^T_{ha,ag} + 1 \text{ and } \beta = b^T_{ha,ag} + 1 \tag{4}$$

Then, ag's trustworthiness according to ha is calculated as the expected value of beta distribution.

$$AT^t_{ha,ag} \overset{\text{def}}{=} E[B | E^T_{ha,ag}] = \frac{\alpha}{\alpha + \beta} \tag{5}$$

2) External Assessment: In this approach, healthcare agent ha seeks information about agent ag from external sources (Figure 2). In our model, we assume that this information can be retrieved from neighboring healthcare agents, $NH = \{ha_1, ha_2, \ldots, ha_n\}$, and from healthcare reputation centres, $HR = \{rp_1, rp_2, \ldots, rp_m\}$; these sources are assumed to be known to ha and are communicated in a secure manner. In this case, we use ha's neighboring healthcare agents' experiences or trustworthiness estimates in addition to ha's internal estimates to calculate the propagated trustworthiness $PT^t_{ha,NH,ag}$ in ag. In addition, we use agent ag's estimated reputation rates $RP^t_{ha,HR,ag}$ that are derived from the patients' feedback about ag. Healthcare agent ha uses this information to strengthen its calculation about ag's trustworthiness $AT^t_{ha,ag}$ by substituting this information in Eq. 6.

$$AT^t_{ha,ag} = \mu PT^t_{ha,NH,ag} + \delta RP^t_{ha,HR,ag}, \quad \text{where } \mu + \delta = 1 \tag{6}$$

Here μ and δ are weighting factors that are set by ha to express the weight it puts on trustworthiness values received from neighboring agents and reputation scores provided by reputation centres. In the following, we show how the calculation is performed for the terms that are expressed in Eq. 6.

a) Propagated trustworthiness: Healthcare agent ha communicates its request about the trustworthiness of agent ag along with its confidence criteria and time scope T to its neighboring agents *NH*. Agents *NH* reply to this request by either providing their recorded experiences with ag or just their trustworthiness estimate that satisfies ha's confidence criteria.

There are three approaches to accommodate *NH*'s feedback and the selection process depends on ha's request's context.

Combined approach: If we assume that each agent $x \in NH$ has a common behaviour, tells the truth, and uses the same evaluation measure as ha, then we add the received experiences from x to ha's self-experiences about ag [6]. Thus, the value of parameters α and β in Eq. 4 will be updated to reflect this change as in Eq. 7.

$$\begin{aligned} \alpha^c &= \sum_{x \in NH \cup \{ha\}} g^T_{x,ag} + 1 \\ \beta^c &= \sum_{x \in NH \cup \{ha\}} b^T_{x,ag} + 1 \end{aligned} \tag{7}$$

As a result, the propagated trustworthiness about ag is calculated as the expected value of the beta distribution as in Eq. 8.

$$PT^t_{ha,NH,ag} = \frac{\alpha^c}{\alpha^c + \beta^c} \tag{8}$$

Discounting approach: If our assumptions in the combined approach are invalid, then we need to use an alternative way to give higher weight to feedback received from highly trusted healthcare agents from ha's perspective. In this approach, we adopt Jøsang et al.'s [6] reputation discounting method that discounts the feedback as a function of the reputation of the healthcare agent who provided it. Therefore, the feedback received from agent x will be adjusted according to ha's previous experiences with x during time T as demonstrated in Eq. 9.

$$\begin{aligned} Dg^T_{ha,x,ag} &= \frac{2g^T_{ha,x}g^T_{x,ag}}{(b^T_{ha,x}+2)(g^T_{x,ag}+b^T_{x,ag}+2)+2g^T_{ha,x}} \\ Db^T_{ha,x,ag} &= \frac{2g^T_{ha,x}b^T_{x,ag}}{(b^T_{ha,x}+2)(g^T_{x,ag}+b^T_{x,ag}+2)+2g^T_{ha,x}} \end{aligned} \tag{9}$$

As a consequence, the values of parameters α and β will change proportionately as expressed in Eq. 10. Thereafter, the propagated trustworthiness is measured as illustrated in Eq. 8.

$$\begin{aligned} \alpha^d &= g^T_{ha,ag} + \sum_{x \in NH} Dg^T_{ha,x,ag} + 1 \\ \beta^d &= b^T_{ha,ag} + \sum_{x \in NH} Db^T_{ha,x,ag} + 1 \end{aligned} \tag{10}$$

Bayesian approach: The discounting approach mandates the need to communicate the anticipated experiences between neighboring healthcare agents *NH* and ha, which would, for example, reveal some information about agent x's interactions with agent ag which may be considered from x's point of view as private information, and thus x may be reluctant to provide this information to ha. To overcome this problem, we use Mui et al.'s [9] Bayesian reputation inference approach where only a trustworthiness estimate is passed between x and ha, which satisfies x's privacy requirements. The propagated trustworthiness in ag as measured by ha through agent x is calculated according to Eq. 11.

$$PAT^t_{ha,x,ag} = AT^t_{ha,x}AT^t_{x,ag} + (1 - AT^t_{ha,x})(1 - AT^t_{x,ag}) \tag{11}$$

We sum the propagated trustworthiness of each $x \in NH$ and normalise it, and then use it to produce ha's propagated trustworthiness in ag as in Eq. 12.

$$PT^t_{ha,NH,ag} = \frac{1}{2}\left(AT^t_{ha,ag} + \frac{\sum_{x \in NH} PAT^t_{ha,x,ag}}{|NH|}\right) \tag{12}$$

b) Reputation Rating: Healthcare agent ha communicates its reputation rating request about agent ag to healthcare reputation centres *HR*. Each reputation centre replies with a value for each rating scale that has been captured during period T, in other words the number of times that ag is rated in each scale. We assume that each $y \in HR$ use the same scale for ratings. Here, we denote the rating scale as a vector $\vec{r} = (r_1, r_2, \ldots, r_k)$; for example, we can use the following rating scale with 5 levels for the healthcare reputation centres, $\vec{r} = (bad, mediocre, average, good, excellent)$. Once centre y has received a reputation rating request about ag, it will reply by sending a vector $\vec{R}^T_{y,ag}$ that contains the associated number for each rating level that has been captured during time period T. Let the rating level be indexed by i and have k levels. Then the aggregate ratings for a particular agent ag are expressed as:

$$\vec{R}^T_{y,ag} = (R^T_{y,ag}(i) | i = 1 \ldots k). \tag{13}$$

In order to calculate the reputation rating score for agent ag, we use Jøsang et al.'s [7] multinomial probability approach where the reputation score is defined as a function of the probability expectation values of each element in $\vec{r}$ at time t. The expectation value for each rating level can be computed with Eq. 14. Let $\vec{R}$ represent ag's aggregated ratings. Then vector $\vec{S}$, defined by,

$$\vec{S}^t_{y,ag} \stackrel{\text{def}}{=} \left(S^t_{y,ag}(i) = \frac{R^T_{y,ag}(i) + Ca(i)}{C + \sum_{j=1}^{k} R^T_{y,ag}(j)} \middle| i = 1 \ldots k \right), \quad \text{where } C = 2 \text{ and } a(i) = \frac{1}{k} \tag{14}$$

is the corresponding multinomial probability reputation score. However, this result does not represent the reputation rating score as a singleton value, so we follow a compacting approach where we assign a weighting factor $v(i)$ to each rating element i as shown in Eq. 15, and, afterwards, we compute the reputation score for ag by multiplying these weights with their corresponding element in $\vec{S}^t_{y,ag}$ and normalise the result as shown in Eq. 16.

$$v(i) = \frac{2i-2}{k-1} - 1, \text{ where } v(i) \in [-1,1] \tag{15}$$

$$RP^t_{ha,y,ag} = \frac{1}{2}\left(\sum_{j=1}^{k} v(j) S^t_{y,ag}(j)\right) + \frac{1}{2} \tag{16}$$

The aforementioned approach shows how a reputation score can be calculated from one healthcare reputation centre y, however, healthcare agent ha might receive feedback from more than one reputation centre and the more feedback we get the more accurate the reputation score we can estimate. There are two approaches to follow in manipulating this feedback and they depend on the reputation centre's behaviour from ha's perspective.

***Combined approach**:* If each $y \in \mathit{HR}$ uses a controlled context in getting the patients' feedback, tells the truth, and uses the same rating framework, then we can combine *HR*'s feedback to represent one vector as in Eq. 17.

$$\vec{\mathit{CR}}^T_{\mathit{HR},ag} \stackrel{\text{def}}{=} \left(\mathit{CR}^T_{\mathit{HR},ag}(i) = \sum_{y \in \mathit{HR}} R^T_{y,ag}(i) \middle| i = 1 \ldots k \right). \tag{17}$$

Subsequently, this vector will be used in Eq. 14 and Eq. 16 to compute the reputation score.

***Bayesian approach**:* It is difficult to assure that healthcare reputation centres *HR* behave equally due to the fact that each centre has its own reputation context that would differ from others. Also, the trustworthiness that ha will have in reputation centre y will vary. In this case, we employ the trustworthiness that ha has in y to relax the reputation score calculated from y's feedback. The trustworthiness is calculated in the same way that we introduced in Section III-A. As a result, we can express the reputation score as in Eq. 18.

$$RP^t_{ha,\mathit{NH},ag} = \frac{1}{2}\left(\sum_{y \in \mathit{RH}} AT^t_{ha,y} \sum_{j=1}^{k} v(j) S^t_{y,ag}(j)\right) + \frac{1}{2} \tag{18}$$

B. Medical Misconduct Practice Evaluation

In the TMDT model, we assume that the healthcare authority creates and maintains a medical misconduct record for each agent ag (a healthcare organisation or a medical practitioner). In order to create and maintain this record, the healthcare authority records malpractice medical cases received from healthcare agents against other agents ag and, afterwards, uses certain classification rules to update the ag's medical misconduct history. We assume that this history is classified in terms of severity and can be presented as a vector $\vec{m} = (m_1, m_2, \ldots, m_n)$, where m_1 denotes the lowest severity and m_n denotes the highest. In this case, each ag has its own medical misconduct record denoted as vector $\vec{M}$, and is expressed as in Eq. 19.

$$\vec{M}_{ag} \stackrel{\text{def}}{=} (M_{ag}(i) | i = 1 \ldots n) \tag{19}$$

In order to estimate ag's medical misconduct rate, the healthcare authority uses a credit deduction process. In this process, each agent ag initially has Z points of credit and this credit is reduced according to ag's reported medical misconduct cases. This deduction process employs a weighting vector $\vec{w}$ that is set by the healthcare authority to determine the credit loss given to each element in $\vec{m}$. Agent ag's (healthcare organisation or medical practitioner) credit is computed as in Eq. 20.

$$AC_{ag} = 1 - \frac{\sum_{i=1}^{n} w(i) M_{ag}(i)}{Z} \tag{20}$$

Now, we can estimate ag's medical misconduct rate as in Eq. 21.

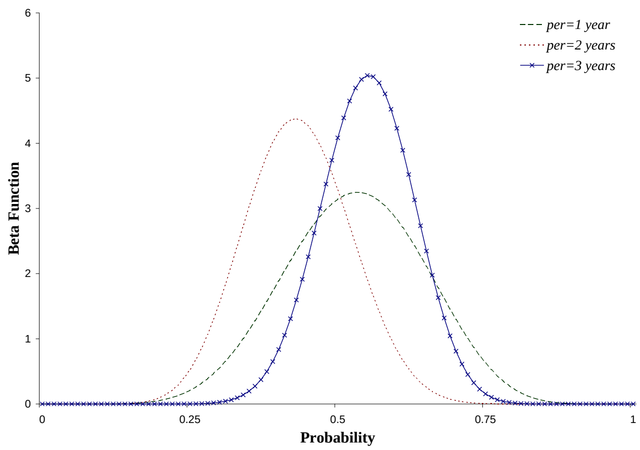
$$\mathit{MR}_{ag} = \begin{cases} AC_{ag}, & \text{where } AC_{ag} \geq 0; \\ 0, & \text{where } AC_{ag} < 0. \end{cases} \tag{21}$$

Thereafter, this value is communicated to ha which substitutes it with the computed trustworthiness values in Eq. 1 to produce the trustworthiness score of the medical data field mdf.

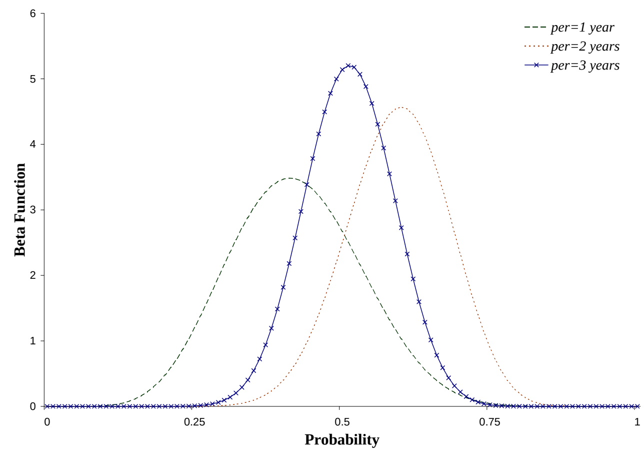
IV. CASE SCENARIO

We use the following case scenario to demonstrate the functionality of the TMDT assessment model and discuss how the chosen time period per can influence our final trustworthiness result. Let's assume that Hospital A's EHR system accesses in 2009 a blood pressure reading b that was created in 2004. The medical reading was entered by Intern K at Hospital J. The EHR system maintains a database where it records its observed experiences with K and J in a time-ordered basis (TABLE II). For the sake of simplicity, we assume that neither K nor J has committed a medical malpractice case, thus $\mathit{MR}_J = \mathit{MR}_K = 1$. Let's assume further that the EHR system sets the confidence criteria $n = 4$ and its subjective weights of the impact of the medical practitioner and healthcare organisation on the medical data's trustworthiness to be $\xi_K = 0.6$ and $\xi_J = 0.4$.

In order to apply Eq. 1, we need to evaluate the trustworthiness of K and J. To carry out that process we need to define the time scope T. Let's assume that $per = 1$, which means one year, so the time scope is defined as $T = [2003, 2005]$. Now, we count Hospital A's good and bad experiences that were recorded during T with both K and J, which leads to the following two binary tuples $E^T_{A,K} = (7, 10)$ and $E^T_{A,J} = (8, 7)$. From these tuples, we notice that the number of A's experiences with either K or J is greater than n. Therefore, we follow the internal assessment approach. Eq. 5 is then used to compute the trustworthiness of K and J to produce trustworthiness measures $AT^t_{A,K} = 0.42$ and $AT^t_{A,J} = 0.52$. These two values thereafter are substituted in Eq. 1 to provide the trustworthiness value of the accessed medical data b which is $T^t_{A,b} = 0.46$.



(a) Hospital J



(b) Intern K

Fig. 3. Beta function of the expected behaviour of the agent

Now let's set the time period per to be 2 years, and follow the aforementioned approach to compute the trustworthiness of blood pressure reading b. We find that the trustworthiness of b gets increased and is equal to 0.51. Let's further change the time period and make per equal 3 years. By following the same approach, we find that Hospital A's trust in b has changed and is now equal to 0.5 which is lower than the second computed value.

Thus, changing the time period affects the final trustworthiness value as it impacts the trustworthiness calculation of the agent. Fig. 3 shows how each chosen period has affected the behaviour of the beta function that is drawn by using the computed α and β values for Hospital J (Fig. 3(a)) and Intern K (Fig. 3(b)) which consequently produced a different trustworthiness value for each time period.

Determining the appropriate size of time period is difficult. For instance, if an agent X's trustworthiness is largely stable over time then in order to evaluate his trustworthiness at a certain time in the past the size of the time period would not make a big difference. However, if the agent X's trustworthiness is unstable and keeps changing, the time period's size will have a high impact on our trustworthiness calculation. Therefore, the appropriate approach to define the time period is to derive it from the agent's recent behaviour.

V. Implementation

To demonstrate the functionality of our model, we have developed a Java application that simulates the relevant part of the functionality of the Electronic Health Record system. Inside the application, we have implemented a trustworthiness service (TS) which implements the TMDT assessment model. Also, we have configured a MySQL database server which the TS uses to get the agent's data required in the trustworthiness calculation process. Each agent's database is represented as a database table in our MySQL server. Also, we built a user interface panel which we use to load the incoming medical data and its metadata and to indicate which external assessment approach the TS will use in cases where the agent's internal experiences fail to satisfy the confidence criteria.

To run our application we set the confidence criteria n and time period per that the TS will use in its trustworthiness evaluation. Upon receiving incoming medical data, which we simulate by entering manually, an evaluation request is sent to the TS which uses the metadata and gets the required internal and, if necessary, external data for trustworthiness calculation process as presented in Section III. Once the TS has finished the calculation, the trustworthiness value is passed to the application which uses the resulting value to change the RGB value of the medical data field's background color to the appropriate red hue to reflect the trustworthiness of the medical data (e.g. dark red indicates untrustworthy data).

VI. Conclusion

An Electronic Health Record (EHR) system overcomes the problems and limitations that are associated with paper based and isolated Electronic Medical Record (EMR) systems; however, its adoption is hindered by concerns over privacy and reliability (trust). Medical data trustworthiness is a vital requirement which has a high impact on how medical data

TABLE II
Hospital A's observed experiences of Hospital J and Intern K

Time	J's observed experiences		K's observed experiences	
	Good	Bad	Good	Bad
1999	1	3	2	1
2000	2	1	1	1
2001	4	0	1	5
2002	3	4	5	1
2003	3	1	1	4
2004	3	1	4	1
2005	2	5	2	5
2006	1	5	2	4
2007	5	1	2	4
2008	1	1	2	1
2009	2	0	3	1

will be utilised. In the current situation, all medical data are usually assumed trustworthy *a priori* so, in the absence of a trustworthiness evaluation, all data will be valued equally; however, this should not be the case.

In this paper, we presented a time-variant medical data trustworthiness model that follows a mathematical statistical approach to conduct trustworthiness evaluations. Our model uses the metadata attached to incoming medical data, namely the healthcare organisation's identity, medical practitioner's identity, and the event timestamp. The trustworthiness evaluation is then conducted by considering the encountered source agent's trustworthiness prior to and after the time at which the medical data was recorded, in order to produce an accurate estimate, rather than relying on the agent's perceived trustworthiness at the current time. Thereafter, the resulting trustworthiness value can be communicated to the EHR displayed on a medical practitioner's computer to alert the medical practitioner to any reliability problems.

In future work we will carry out an investigation to define the time period as a function of the agent's trustworthiness behaviour. Also, we plan to demonstrate this model by implementing it in a healthcare workflow system. We plan to implement TMDT as a service within the YAWL[4] system where it will respond to each reliability assessment request that comes from any healthcare workflow process. Finally, we plan to utilise the metadata attributes that are employed by YAWL to reflect the calculated reliability score of a given medical data.

Acknowledgment

The first author's work is gratefully sponsored by King Saud bin Abdulaziz University for Health Sciences – Saudi Arabia.

References

[1] B. Blobel, "Authorisation and Access Control for Electronic Health Record Systems," *International Journal of Medical Informatics Realizing Security into the Electronic Health Record*, vol. 73, no. 3, pp. 251–257, 2004.

[2] D. Denison, C. Holmes, B. Mallick, and A. Smith, *Bayesian Methods for Nonlinear Classification and Regression*. Wiley, 2002.

[3] T. Deursen, P. Koster, and M. Petkovic, "Hedaquin: A Reputation-based Health Data Quality Indicator," *Electronic Notes in Theoretical Computer Science*, vol. 197, no. 2, pp. 159–167, February 2008.

[4] T. D. Gunter and N. P. Terry, "The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions," *Journal of Medical Internet Research*, vol. 7, no. 1, p. e3, 2005.

[5] I. Iakovidis, "Towards Personal Health Record: Current Situation, Obstacles and Trends in Implementation of Electronic Healthcare Record in Europe," *International Journal of Medical Informatics*, vol. 52, no. 1–3, pp. 105–115, 1998.

[6] R. Ismail and A. Jøsang, "The Beta Reputation," in *Proceedings of the* 15^{th} *Bled Electronic Commerce Conference, Bled, Slovenia, June 17–19*, 2002.

[7] A. Jøsang and J. Haller, "Dirichlet Reputation Systems," in *Proceedings of the* $2nd$ *International Conference on Avialability, Reliability and Security (ARES 2007), Vienna, Austria, April 10–13*. IEEE, 2007.

[8] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," in *Proceedings of the* 12^{th} *international conference on World Wide Web 2003, Budapest, Hungary, May 20–24*. New York, NY, USA: ACM, 2003, pp. 640–651.

[9] L. Mui, M. Mohtashemi, C. Ang, P. Szolovits, and A. Halberstadt, "Rating in Distributed Systems: A Bayesian Approach," in *Proceeding of the* 11^{th} *Workshop on Information Technologies and Systems (WITS 2001), New Orleans, Louisiana, December 15–16*, 2001.

[10] P. Resnick and R. Zeckhauser, "Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System," in *The Economics of the Internet and E-commerce*, ser. Advances in Applied Microeconomics, M. R. Baye, Ed. Emerald Group Publishing Limited, 2002, vol. 11, pp. 127–157.

[11] J. Schneider, G. Kortuem, J. Jager, S. Fickas, and Z. Segall, "Disseminating Trust Information in Wearable Communities," *Personal Ubiquitous Computing*, vol. 4, no. 4, pp. 245–248, 2000.

[12] W. Teacy, J. Patel, N. Jennings, and M. Luck, "TRAVOS: Trust and Reputation in the Context of Inaccurate Information Sources," *Autonomous Agents and Multi-Agent Systems*, vol. 12, no. 2, pp. 183–198, 2006.

[13] L. Xiong and L. Liu, "A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communication," in *Proceedings of the IEEE international Conference on E-Commerce (CEC'03), Newport Beach, California, June 24-27*, J.-Y. Chung and L.-J. Zhang, Eds. IEEE, 2003.

[14] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-based Trust for Peer-to-Peer Electronic Communities," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843–857, July 2004.

[4]http://www.yawl-system.com/